

WHAT IS CLAIMED IS:

Claim 1:

1. A method for use with a computer system having an Internet visible web server accessible to a web browser for sending response messages fulfilling calls from said web browser by sending back to said web browser an item requested in said calls, the method comprising:
- a. transmitting a received call from said Internet visible web server to an Gateway CGI (Gateway CGI),
 - b. transferring, via said Gateway CGI, Internet visible Web server the call to an Gateway CGI program,
 - c. extracting and packaging said call by said Gateway CGI program into an Encoded Request Package (ERP) with sufficient information to reconstruct the call,
 - d. establishing, via said Gateway CGI, a socket to communicate with an instance of a second server (hereinafter an ACM) in a secure part of said computer system,
 - e. transmitting information embodied in the original request in said ERP to said ACM,
 - f. reconstructing said call by said ACM,
 - g. attempting to verify access privileges for said call,
 - h. if access privileges are verified, retrieving, by said ACM, said item requested by said call,
 - i. forwarding said item to said Internet visible web server,
 - j. sending said item to said Gateway CGI across said socket,
 - k. serving said item in a message to said web browser from said Internet visible web server.

Claim 2:

- 1 2. The method of Claim 1 wherein transmitting step "a." occurs within a
2 single computer system.

Claim 3:

- 1 3. The method of Claim 1 wherein said establishing step "d." occurs by first
2 signaling from said Gateway CGI to a Daemon in said secure part of said
3 computer system across an establishment socket to which said Daemon is
4 attuned, establishing an instance of said ACM by said Daemon and attaching
5 said ACM to a communications socket through which all further communication
6 between said ACM and Gateway CGI shall occur.

Claim 4:

- 1 4. The method of claim 3 wherein said signaling and said all further
2 communications is encrypted.

Claim 5:

- 1 5. The method of claim 3 wherein said signaling does not contain an ERP.

Claim 6:

- 1 6. The method of claim 3 wherein said signaling does contain an ERP and
2 wherein said establishing of an instance of said ACM by said Daemon includes
3 transfer of said ERP to said ACM.

Claim 7:

- 1 7. The method of Claim 1 wherein in step "g." wherein the ACM does the
2 verification and if the ACM fails to verify the call, the ACM terminates.

Claim 8:

1 8. The method of Claim 1 wherein in step "g." wherein the ACM does the
2 verification and if the ACM fails to verify the call, the ACM returns a request for a
3 log-on.

Claim 9:

1 9. The method of claim 8 wherein the ACM embeds user request information
2 in the logon request.

Claim 10:

1 10. The method of Claim 1 wherein in step "g." wherein the ACM does the
2 verification and if the ACM fails to verify the call, the ACM communicates this
3 failure to said Gateway CGI and awaits further verification information.

Claim 11:

1 11. The method of Claim 1 wherein said step "h." includes activating a CGI on
2 said secure system.

Claim 12:

1 12. A method for operating a web server comprising:
2 establishing an internet visible web server (hereinafter IVWserver)
3 to receive calls from web browsers on the internet,
4 receiving said calls,
5 relaying said calls to an Gateway CGI on a same computer system
6 with said IVWserver,
7 packaging information from said calls into an Encoded Request
8 Packet (ERP) sufficient to reconstruct said calls from said ERP,
9 establishing a communication channel between said Gateway CGI
10 and an Access Control Management (ACM) program on said secure
11 computer system,

12 authenticating the call,
13 sending the ERP to said ACM program,
14 reconstructing the call by said ACM program,
15 executing the call by the ACM program,
16 sending a result from said call execution to said Gateway CGI,
17 providing said result to said IVWserver,
18 sending said result to said web browser.

Claim 13:

1 13. The method of claim 12 wherein said receiving step comprises, receiving
2 a call at a dispatcher, selecting a one of a set of IVWservers by said dispatcher,
3 and sending said call to said selected one by said dispatcher.

Claim 14:

1 14. The method of Claim 12 wherein said establishing occurs by first signaling
2 from said Gateway CGI to a Daemon in said secure computer system across an
3 establishment socket to which said Daemon is attuned, establishing an instance
4 of said ACM program by said Daemon and attaching said ACM to a
5 communications socket through which all further communication between said
6 ACM and Gateway CGI shall occur.

Claim 15:

1 15. The method of claim 14 wherein said Daemon signals said Gateway CGI
2 information regarding the communications socket.

Claim 16:

1 16. The method of Claim 12 wherein said executing includes activating a CGI
2 on said secure computer system.

Claim 17:

1 17. The method of claim 16 wherein said activated CGI is a session controller
2 for a database and wherein said session controller maintains an open session for
3 a user to use data in a working database.

Claim 18:

1 18. The method of claim 17 wherein said working database is not located on
2 said secure computer system but on an intranet and said session controller
3 maintains an open session through an intranet firewall.

Claim 19:

1 19. The method of Claim 12 wherein said authenticating requires matching of
2 information transferred by the web browser to expected information.

Claim 20:

1 20. The method of Claim 19 wherein a session controller further authenticates
2 the call.

Claim 21:

1 21. The method of claim 19 wherein said secure computer system maintains a
2 user database for containing at least some of said expected information.

Claim 22:

1 22. The method of Claim 12 wherein said executing includes retrieving files,
2 including those file types in the set {HTML, image, data} from said secure
3 computer system.

Claim 23:

1 23. The method of Claim 12 comprising a step prior to said establishing an
2 IVWserver to receive calls from web browsers on the internet wherein said prior
3 step comprises:

4 receiving at a dispatcher all calls from web browsers, and
5 routing each received call to an available IVWserver in a pool of
6 IVWservers.

Claim 24:

1 24. The method of Claim 12 wherein said step of establishing a
2 communication channel between said Gateway CGI and an ACM program on
3 said secure computer system comprises:

4 contacting a Daemon on said secure computer system by said Gateway
5 CGI,

6 sending a request for an ACM to said Daemon by said Gateway CGI
7 spawning an ACM by said Daemon,

8 sending port information to said Gateway CGI from said Daemon to
9 indicate on which port said ACM will communicate with said Gateway CGI.

Claim 25:

1 25. A networked computer system having at least two zones, an Internet
2 visible zone and a secure internal zone, wherein secure data is located on said
3 secure zone but can be made available to a web browser which can
4 communicate with said Internet visible zone by sending calls through an internet
5 network to said Internet visible zone and wherein said web browser can receive
6 messages through said internet network from said Internet visible zone, said
7 networked computer system comprising:

8 a first computer system having a web server for receiving at least
9 one of said calls from said web browser and serving said web browser
10 with messages through said internet network,

11 a Gateway CGI program for receiving a call from said web browser,
12 said Gateway CGI program having program elements to extract
13 identification information and URL information from said call, having a
14 packaging program to produce an Encoded Request Package (ERP) from
15 said call and having a connection element for sending said ERP to a web
16 server-like Access Control Manager (ACM) in said internal zone,

17 said ACM in said secure internal zone having a program for
18 receiving said ERP, a program for converting said ERP into a call, a
19 program for authenticating said ERP, and a program for retrieving
20 information available to said ACM within said internal zone and for
21 sending said information to said Gateway CGI.

Claim 26:

1 26. A networked computer system as set forth in Claim 25, wherein said
2 Gateway CGI connection element has a signal generating means for sending a
3 ready signal to a Daemon port in said secure internal zone that it is ready to send
4 an ERP, and wherein said secure internal zone has a Daemon program for
5 monitoring said Daemon port for such ready signals, and wherein said Daemon
6 further comprises a generating process for spawning an ACM.

Claim 27:

1 27. A networked computer system as set forth in Claim 26, wherein said
2 generating process further comprises reassignment program for connecting said
3 ACM to a communications port.

Claim 28:

1 28. A networked computer system as set forth in Claim 27, wherein said
2 reassignment program further comprises Gateway CGI communications process
3 for sending a message to said Gateway CGI to indicate that said ACM has been
4 assigned to said communications port.

Claim 29:

1 29. A networked computer system as set forth in Claim 25, further comprising
2 a dispatcher unit and wherein said first computer system is a pool of computers,
3 each having a web server and a Gateway CGI.

Claim 30:

1 30. A networked computer system as set forth in Claim 25, wherein said ACM
2 program for retrieving information comprises program means for sending said
3 call to a CGI in said secure zone.

Claim 31:

1 31. A networked computer system as set forth in Claim 25, wherein said ACM
2 program for retrieving information comprises program means for retrieving data
3 requested in said call from said secure zone.

Claim 32:

1 32. A first web server in a computer system in an internet visible zone having
2 configuration rules set to establish that substantially all calls received from web
3 browsers are sent to a specific CGI, wherein that specific CGI is a gateway CGI
4 for communicating with a second web server, said gateway CGI comprising:

- 5 a. receiving process for receiving a said call sent by said web server,
- 6 b. extracting process for extracting user and environmental
7 identification information to produce an identification extraction, and
8 for reproducing URL information from said call,
- 9 c. packaging process for producing a data package having said
10 identification extraction and said URL information,
- 11 d. sending process for sending said data package to a second web
12 server in a second zone,
- 13 e. receiving process for receiving a reply message from said second
14 web server, and

- 15 f. reply process for sending said reply message to said first web
16 server in said internet visible zone.

Claim 33:

- 1 33. A gateway CGI for use in a first web server in a computer system in an
2 internet visible zone having configuration rules set to establish that substantially
3 all calls received from web browsers are sent to a gateway CGI for
4 communicating with a second web server, said gateway CGI comprising:
5 a. receiving process for receiving a said call sent by said web server,
6 b. extracting process for extracting user and environmental
7 identification information to produce an identification extraction, and
8 for reproducing URL information from said call,
9 c. packaging process for producing a data package having said
10 identification extraction and said URL information,
11 d. sending process for sending said data package to a second web
12 server in a second zone,
13 e. receiving process for receiving a reply message from said second
14 web server, and
15 f. reply process for sending said reply message to said first web
16 server in said internet visible zone.

Claim 34:

- 1 34. A gateway CGI as set forth in claim 33 wherein said sending process
2 comprises signaling process for establishing a communications socket through
3 which to communicate with said second web server.

Claim 35:

- 1 35. A gateway CGI as set forth in claim 33 wherein said sending process
2 comprises encryption process for encrypting said package.

Claim 36:

- 1 36. A gateway CGI as set forth in claim 35 wherein said receiving process
2 comprises decryption process for decrypting said reply message.

Claim 37:

- 1 37. A gateway CGI as set forth in claim 33 wherein said sending process
2 comprises signaling process for establishing a communications socket through
3 which to communicate with said second web server.

Claim 38:

- 1 ^{Res} 38. An Access Control Manager (ACM) program for retrieving secure
2 ^{SW} information from within a secure zone and sending said secure information to an
3 internet visible zone, said ACM program comprising:
4 means for receiving a data package containing call information in a
5 packaged form comprising call identification information signals and URL
6 identifying signals,
7 means for unpacking said data package and reconstituting a call
8 from said call information,
9 Web server means to act on said call and produce a reply.

Claim 39:

- 1 ^{Res} 39. A secure zone computer system comprising:
2 ^{SW} at least two ports for forming socket connections to a first web
3 server program on an internet visible zone,
4 a monitoring Daemon for monitoring a first of said two ports for
5 gateway CGI communications and for spawning an Access Control
6 Manager and assigning said Access Control Manager to a second of said
7 two ports for enabling socket communications between said Access
8 Control Manager and said gateway CGI.